



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,225	09/10/2003	Paul M. Agbabian	SYMC1001	7712
34350 7590 12/19/2007 GUNNISON, MCKAY & HODGSON, L.L.P. 1900 GARDEN ROAD, SUITE 220 MONTEREY, CA 93940			EXAMINER HOFFMAN, BRANDON S	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 12/19/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/660,225

Applicant(s)

AGBABIAN, PAUL M.

Examiner

Brandon S. Hoffman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-18 are pending in this office action.

Claim Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

3. Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Li et al. (U.S. Patent Pub. No. 2004/0193912).

Regarding claim 1, Li et al. teaches a system comprising a security management system comprising:

- A network security feedback and control system wherein said security feedback and control system receives a plurality of normalized events and issues at least one normalized command in response to a predefined event in said plurality of normalized events (paragraph 0022-0023).

Regarding claim 2, Li et al. teaches wherein said security feedback and control system comprises a feedback and control manager wherein said feedback and control

manager processes said at least one normalized event and generated said at least one normalized command (fig. 3, ref. num 340).

Regarding claims 3 and 13, Li et al. teaches wherein said feedback and control manager includes at least one rules engine wherein said rules engine includes a rule having a condition object that uses information from said at least one normalized event (fig. 3, ref. num 350).

Regarding claim 4, Li et al. teaches further comprising a managed node coupled to said security management system (fig. 1, ref. num 113).

Regarding claim 5, Li et al. teaches wherein said managed node further comprises a security management agent executing on said management node (fig. 1, ref. num 120).

Regarding claim 6, Li et al. teaches further comprising at least one managed product coupled to said security management agent wherein said at least one managed product forwards at least one of said normalized events to said security management agent and receives normalized commands from said security management agent (fig. 2, ref. num 254).

Regarding claims 7 and 14, Li et al. teaches further comprising a security management agent coupled to said network security feedback and control system wherein said security management agent collects normalized events and forwards said normalized events to said security management system (fig. 2, ref. num 254).

Regarding claims 8 and 15, Li et al. teaches further comprising at least one managed product coupled to said security management agent wherein at least one managed product transfers at least one normalized event to said security management agent (fig. 2, ref. num 240).

Regarding claim 9, Li et al. teaches a system comprising:

- An event subscription filter, **said event subscription filter for receiving a plurality of normalized events from managed products and for passing normalized events, for which said system is registered, to a feedback and control manager** (fig. 2, ref. num 220); and
- A feedback and control manager coupled to said event subscription filter, **wherein said feedback and control manager processes at least one normalized event received from said event subscription filter and issues at least one normalized command for use in dynamically implementing a predefined security policy** (fig. 2, ref. num 240 and paragraph 0022-0023).

Regarding claim 10, Li et al. teaches further comprising a knowledge database coupled to said feedback and control manager (paragraph 0013).

Regarding claim 11, Li et al. teaches further comprising a directory coupled to said feedback and control manager (paragraph 0013).

Regarding claim 12, Li et al. teaches further comprising a configuration adapter connected between said feedback and control manager and said directory (fig. 1, POLICY DATA INTERFACE).

Regarding claims 16-18, Li et al. teaches a method/computer-program product/structure comprising:

- Receiving a **plurality of normalized** events from managed products by a network security feedback and control system (fig. 2, ref. num 230 and 240); and
- Using information in said **plurality of normalized** events by said network security feedback and control system in dynamically implementing a predefined security policy **by issuing at least one normalized command in response to a predefined event in said plurality of normalized events** (fig. 2, ref. num 250 and 252 and paragraph 0022-0023).

Response to Arguments

4. Applicant argues Li et al. does not teach issuing a normalized command in response to a predefined event in said plurality of normalized events (page 6 and page 7).

Regarding applicant's argument, examiner disagrees. Examiner looked at the claim language to determine what a normalized event and normalized command was and could not find a description. Examiner next looked to the specification, page 17, and found out that a normalized event was a hierarchical structure that includes at least a base security event, so that security and feedback control system 155 is extensible; a normalized command was provided to appropriate products in system 100 to implement the security policy embedded in security feedback and control system 155. With that definition, Li et al. reads on the claim limitations. Specifically, the claims call for receiving a normalized event, and in response, issuing a normalized command. Li et al, at paragraph 0022, teaches receiving normalized events. These events are security threats, which are normalized by the PFP 120. In response to these security threats, or events, Li et al. further teaches that alerts and notifications (commands) are sent to the appropriate personnel suggesting changes (end of paragraph 0022), and based on the detection of a specific threat, SQL Slammer, a revised policy is issued (a command) to temporarily deny port access (paragraph 0024).

The other independent claims were amended to match claim 1 and are rejected for the same reasons as independent claim 1.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


12, 17, 07